FORRESTER®

Technology Adoption Profile personnalisé pour Dell | Octobre 2017

Sécurité évolutive adaptée à l'employé moderne

DÉMARRER ▶

Technology Adoption Profile personnalisé pour Dell | Octobre 2017

Sécurité évolutive adaptée à l'employé moderne

La sécurité doit protéger et habiliter les employés

Afin de tenir le rythme de la croissance de la mobilité des entreprises, en évitant ses risques potentiels, le service informatique doit être capable de traiter efficacement les problèmes complexes, allant de la prestation de services, à l'acquisition d'appareils, en passant par la surveillance de la sécurité. Pourquoi cela ? Les travailleurs de l'information ont besoin d'accéder à des informations souvent sensibles sur une grande diversité d'applications métier et d'appareils, où qu'ils soient. En d'autres termes, les politiques de sécurité et de confidentialité qui ne nuisent pas à la productivité des utilisateurs finaux permettront d'habiliter les employés, tout en optimisant leurs performances.

CONTEXTE DU PROJET

En juillet 2017, Dell a demandé à Forrester de réaliser une étude sur les employés du XXIe siècle et sur la façon dont leurs nouvelles habitudes, attitudes et méthodes de travail modifient le monde du travail. Compte tenu du nombre plus élevé de profils à satisfaire dans une seule société, les entreprises ne parviennent pas à répondre aux demandes des employés. Pour accomplir leurs tâches, les employés contournent les politiques de sécurité pour obtenir ce qu'ils veulent, lorsqu'ils en ont besoin. Les entreprises doivent comprendre les différents comportements des employés et équilibrer soigneusement et équitablement les besoins de sécurité, sous peine de s'exposer à des menaces, nouvelles et existantes, sans précédent.

Pays

- Australie : **25 %**
- Inde : **25 %**
- États-Unis : **25 %**
- Royaume-Uni : **25 %**

Type d'entreprise

- Locales : **11 %**
- Régionales : **35 %**
- Multinationales : **54 %**

Chiffre d'affaires annuel (USD)

- Entre 400 et 499 millions USD : **21 %**
- Entre 500 et 999 millions USD : **31 %**
- Entre 1 et 5 milliards USD : **28 %**
- > 5 milliards : **20 %**

Types de profils

- Employés de bureau : Personnel de bureau : **32 %** et Arpenteur de couloirs : **23 %**
- Employés ne travaillant pas dans un bureau : Professionnel mobile : **24 %** Travailleur à distance : **22 %**
- **Rôle spécialisé :** Employés chargés de la propriété intellectuelle : créatif : **30 %** et ingénieur : **24 %**

Sécurité évolutive adaptée à l'employé moderne

Les employés diversifiés d'aujourd'hui utilisent de nombreux appareils

La numérisation du lieu de travail permet aux travailleurs de l'information d'obtenir ce qu'ils veulent, lorsqu'ils en ont besoin. L'époque ou un employé dévoué se rendait et quittait le même lieu de travail chaque jour de la semaine est révolue. L'omniprésence des technologies mobiles, des politiques de travail flexibles et des préférences des employés implique que le personnel numérique actuel travaille à domicile, dans des lieux publics et depuis différents endroits. Les travailleurs de l'information utilisent également une grande variété d'appareils. Le défi posé aux services informatiques, consiste à permettre aux employés d'utiliser ces appareils en toute sécurité, de manière à respecter leurs propres protocoles de sécurité, tout en améliorant l'efficacité et la réussite de l'entreprise, sans nuire à l'autonomie ou à la productivité des employés.

Aux fins de cette étude, nous avons défini les types d'employés suivants :

- **Employés de bureau :** personnel de bureau et arpenteurs de couloirs.
- **Employés ne travaillant pas dans un bureau :** les travailleurs à distance et les professionnels mobiles.
- **Employés chargés de la propriété intellectuelle :** créatifs et ingénieurs.

Les ordinateurs portables restent l'appareil le plus populaire parmi tous les types d'employés, dont 57 % les utilisent pour effectuer leur travail, peu importe leur lieu de travail.

« Où utilisez-vous les appareils suivants pour le travail au cours d'une semaine type ? »

	Travailleur à distance	Professionnel mobile	Personnel de bureau	Arpenteur de couloir	Créatif	Ingénieur
Tout type d'ordinateur de bureau	58 %	45 %	67 %	63 %	58 %	53 %
Tout type de portable	69 %	50 %	63 %	38 %	61 %	63 %
Tout type de 2-en-1/« convertible » avec des écrans tactiles et des écrans pivotants	26 %	34 %	17 %	23 %	33 %	38 %
Tout type d'espace de travail partagé	20 %	28 %	16 %	22 %	31 %	19 %
Tout type d'affichage ad hoc pour la collaboration	19 %	20 %	17 %	12 %	24 %	20 %
Tout type de stockage de données portable et d'accessoires	21 %	34 %	26 %	21 %	36 %	32 %
Tous types de tablettes de 7 à 12 pouces	17 %	35 %	20 %	18 %	27 %	28 %
Téléphone portable	13 %	22 %	6 %	6 %	15 %	14 %
Smartphone	56 %	64 %	57 %	41 %	70 %	59 %
Appareil connecté mobile spécifique à un objectif	10 %	16 %	5 %	18 %	9 %	10 %

Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

Sécurité évolutive adaptée à l'employé moderne

1 2 3

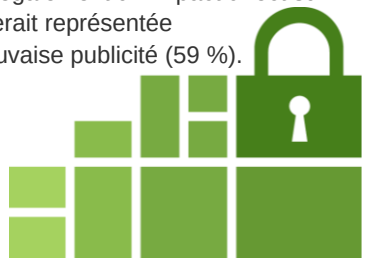
Les employés estiment que les processus de sécurité de leur entreprise sont réactifs

Les données sont la pierre angulaire des entreprises numériques actuelles. Leur protection contre le vol, le mauvais usage et la violation constitue une priorité absolue pour les organisations du monde entier, d'autant plus que les sociétés n'ont pas besoin de chercher bien loin, ni même de suivre les actualités pour savoir que les menaces pesant sur l'intégrité des données sont endémiques.

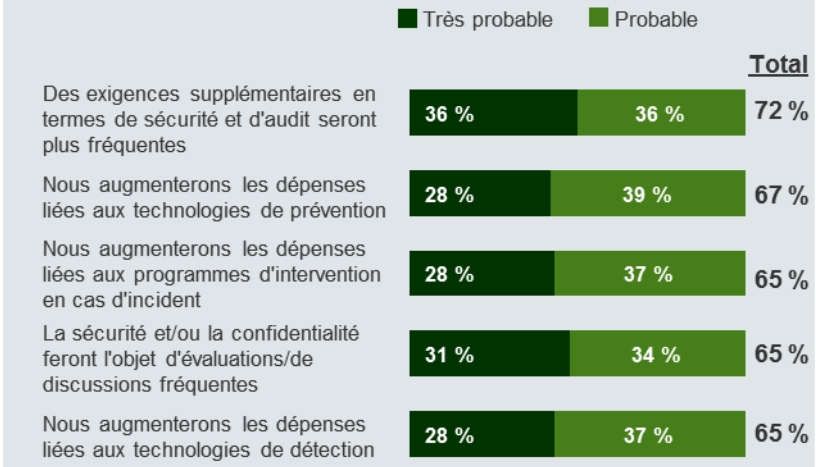
Les travailleurs de l'information ont révélé que si une violation de sécurité se produisait, celle-ci entraînerait davantage de dépenses, de projets de sécurité et d'exigences. Par exemple, les personnes interrogées ont déclaré que si une violation de sécurité se produisait, on constaterait alors une augmentation des exigences en matière de sécurité et d'audit (72 %), une hausse des dépenses liées à la prévention (67 %) et un accroissement des dépenses en technologies de détection (65 %).

De plus, une violation de la sécurité attirerait non seulement l'attention de l'ensemble de l'organisation, mais aurait également un impact direct sur l'entreprise, en ce sens que la marque serait représentée négativement (62 %) et attirerait une mauvaise publicité (59 %).

82 % des travailleurs de l'information ont qualifié la réponse de leur entreprise à une violation de sécurité de très réactive ou réactive.



« Quelle serait les répercussions les plus probables en cas, ou suite à un événement de violation de sécurité ? » (Seules les cinq premières propositions « Très probable » et « Probable » sont affichées)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

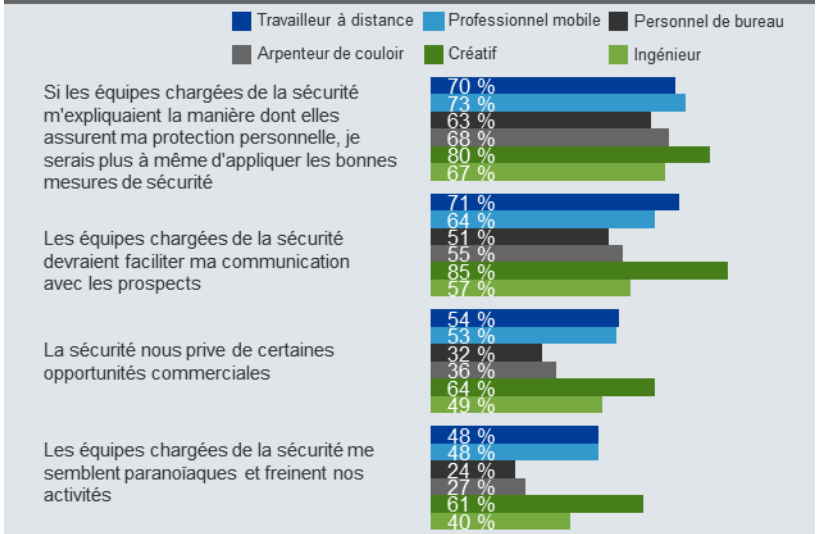
Sécurité évolutive adaptée à l'employé moderne

L'encadrement (et non un contrôle assidu) mène à de meilleures pratiques de sécurité

Les organisations ont du mal à comprendre qui sont leurs employés et comment gérer la grande diversité des types de travailleurs d'aujourd'hui. Tous les types d'employés sont entièrement d'accord ou d'accord sur le fait que les équipes chargées de la sécurité devraient expliquer la manière dont elles assurent leur protection, afin qu'ils soient plus à même d'appliquer de bonnes pratiques de sécurité.

Cependant, certaines variations intéressantes émergent à travers les différents profils. Les employés ne travaillant pas dans un bureau (54 % en moyenne) et les professionnels chargés de la propriété intellectuelle (57 % en moyenne) ont déclaré que la sécurité les privaient de certaines opportunités commerciales et que la communication entre les employés et les prospects devrait être facilitée. De plus, les équipes chargées de la sécurité doivent être en mesure de soutenir et même d'accélérer l'utilisation des différents appareils parmi les employés. Toutefois, les employés ne travaillant pas dans un bureau et les professionnels chargés de la propriété intellectuelle ont déclaré avoir des difficultés à collaborer avec les équipes chargées de la sécurité : qu'ils rencontrent des paranoïaques et que ceux-ci nuisent à leurs activités.

« À quel point êtes-vous d'accord avec les affirmations suivantes concernant les équipes chargées des protocoles de sécurité sur les appareils que vous utilisez pour travailler ? (Seules les réponses « Entièrement d'accord » et « D'accord » sont affichées)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

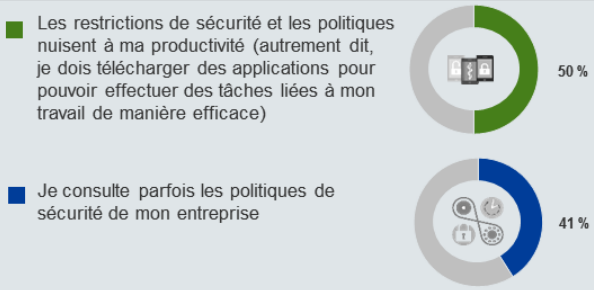
Sécurité évolutive adaptée à l'employé moderne

Les employés sont contrariés par les politiques de leur propre entreprise

Les employés essaient d'effectuer leur travail, mais leur efficacité est compromise par les contrôles de sécurité, car ceux-ci sont mal conçus et ne sont pas assez dynamiques pour satisfaire les différents profils et répondre à leurs besoins. C'est pourquoi, la moitié (50 %) des travailleurs de l'information ont déclaré que les restrictions et les politiques de sécurité compromettaient leur productivité, et 41 % ont indiqué qu'ils consultaient parfois les politiques de sécurité de l'entreprise.

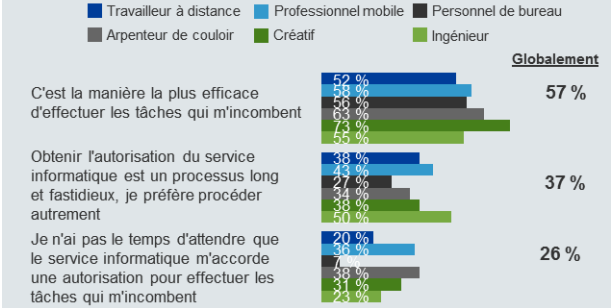
En d'autres termes, les employés choisissent la solution de facilité pour faire avancer les choses, car il s'agit du moyen le plus efficace (57 %). Les employés ont besoin d'accéder à des informations d'entreprise sensibles à partir de leurs appareils, et obtenir l'autorisation du service informatique est un processus long et fastidieux (37 %). Il est intéressant de noter que les employés ne travaillant pas dans un bureau et les professionnels chargés de la propriété intellectuelle sont plus susceptibles d'enfreindre le protocole de sécurité pour obtenir ce dont ils ont besoin. Par exemple, 75 % des professionnels mobiles et des professionnels chargés de la propriété intellectuelle, ainsi que des ingénieurs (49 %) et les créatifs (52 %), sont plus susceptibles d'enfreindre les politiques de sécurité. Par conséquent, les entreprises doivent se concentrer sur ceux-ci, étant donné qu'ils causent le plus de problèmes.

« À quel point êtes-vous d'accord avec ce qui suit ? » (Les réponses « Entièrement d'accord » et « D'accord » sont affichées en même temps)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

« Pourquoi consultez-vous parfois les politiques de sécurité de votre entreprise ? » (Sélectionnez toutes les réponses appropriées)



Panel : variable ; travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

Sécurité évolutive adaptée à l'employé moderne

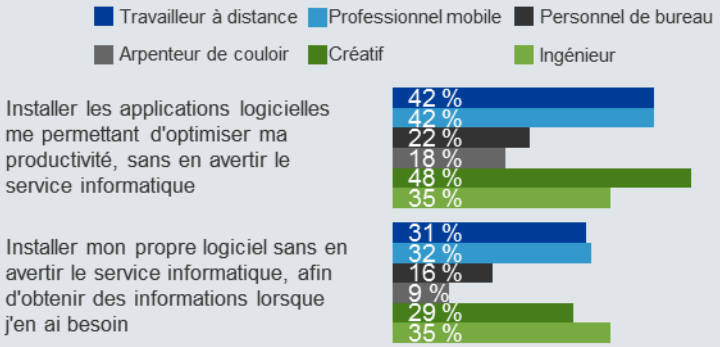
Les employés aspirent à la productivité, sans intention malveillante

Les employés souhaitent accéder aux logiciels et aux applications leur permettant d'effectuer leur travail. Si les équipes chargées de la sécurité leur imposent trop de politiques et de contrôles, comme la nécessité d'obtenir une autorisation d'accès à une application ou un téléchargement de logiciel, les employés rechercheront activement des alternatives provenant d'autres sources. Ils contourneront les processus de sécurité, sans en avertir le service informatique, en augmentant les risques de sécurité. Toutefois, l'intention des employés n'est pas malveillante. Ils ont besoin d'accéder aux applications et aux logiciels à des moments particuliers, afin de pouvoir être productifs.

Il n'est pas surprenant que les employés de bureau (personnel de bureau et arpenteurs de couloirs) soient moins susceptibles d'installer des logiciels ou des applications sans en avertir le service informatique, comparé à leurs homologues ne travaillant pas dans un bureau (travailleurs à distance et professionnels mobiles) et ceux chargés de la propriété intellectuelle (créatifs et ingénieurs). Ils sont plutôt plus susceptibles de faire ce qu'ils veulent si cela implique qu'ils peuvent être productifs, tout en étant en mesure d'accéder aux informations lorsqu'ils en ont besoin, où qu'ils soient.

Il existe des lacunes évidentes en matière de sécurité : *62 % des travailleurs à distance craignent d'être blâmés pour une violation ou un événement de sécurité. Les ingénieurs craignent de provoquer des fuites de données client (73 %), toutefois, ils estiment devoir installer des applications pour améliorer leur productivité sans en avertir le service informatique.*

« Comment allez-vous procéder pour obtenir le logiciel dont vous avez besoin pour être productif ? »
(Sélectionnez une seule réponse)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

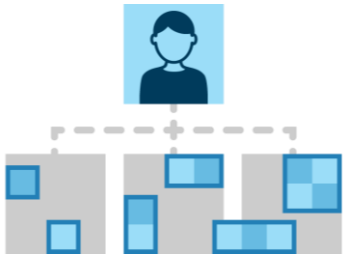
Sécurité évolutive adaptée à l'employé moderne

Les employés ont besoin de partager des données : le service informatique doit les habiliter en toute sécurité

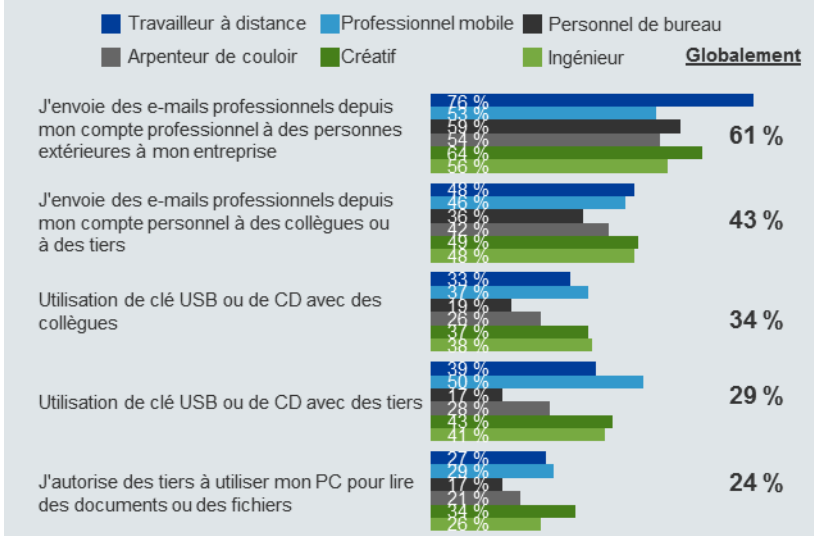
Au XXIe siècle, l'économie de données est une notion essentielle pour comprendre que les données ont une vie propre. Les organisations collectent des tonnes de données, en complexifiant la protection de celles-ci, en raison de la quantité de données générées par les utilisateurs finaux, puis stockées et dupliquées dans divers endroits, tels que le cloud, les clés USB, etc.

En dépit de la connaissance des conséquences et des répercussions d'une violation de sécurité, les employés souhaitent, doivent et continueront de partager des données avec leurs collègues ou des entreprises tierces. Cependant, les employés partagent des informations dans des environnements non sécurisés, en exposant leur entreprise à des risques. Les professionnels de la sécurité doivent trouver des solutions pour répondre aux besoins des différents profils d'aujourd'hui, d'une manière beaucoup plus sécurisée, facilement accessible et simple d'utilisation.

71 % des employés ont déclaré partager des fichiers avec des tiers, tous les jours ou toutes les semaines.



« Comment procédez-vous pour partager des documents ou des fichiers avec des tiers ? » (Sélectionnez toutes les réponses appropriées)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

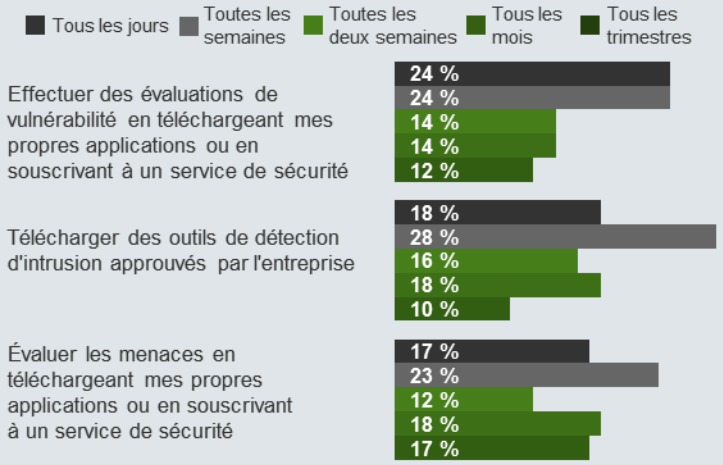
1 2

Compte tenu de l'autorité et des outils, les employés s'approprieraient le domaine de la sécurité

Il est évident que les approches actuelles en matière de sécurité sont extrêmement fragmentées en fonction des différents types d'employés. Les employés apprécient la sécurité, mais ils souhaitent que celle-ci interfère moins dans leurs tâches quotidiennes. Moins la sécurité est intrusive et plus les employés s'y conformeront. Mais si le service informatique nuit à leur productivité avec des processus d'authentification ou s'il leur impose des restrictions sur certaines applications et certains outils leur permettant d'effectuer correctement leur travail, les employés se montreront réticents à l'égard des consignes de sécurité.

Toutefois, les employés comprennent également que la sécurité n'est pas une tâche facile, leur attitude change et ils font preuve d'empathie envers les équipes chargées de la sécurité. Ceci explique pourquoi, les employés effectueraient des évaluations de vulnérabilité au moins une fois par mois s'ils en avaient la possibilité. L'objectif est de trouver le juste milieu entre donner trop de contrôle aux employés et imposer des politiques de sécurité moins intrusives. L'intégration de la protection des fichiers au flux naturel des processus métiers et l'installation d'une protection contre les logiciels malveillants sont essentielles pour permettre aux employés d'être productifs et d'effectuer leur travail en toute sécurité. Diverses solutions de sécurité peuvent tirer parti de ces données comportementales pour corréler les menaces potentielles sur d'autres couches (terminal, réseau, physique/géographique) ou prendre des décisions plus éclairées sur le risque d'une transaction ou d'un comportement donné(e).

« Si vous supervisiez la gestion de votre propre sécurité, à quelle fréquence effectuerez-vous les actions suivantes ? »



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

Sécurité évolutive adaptée à l'employé moderne

1 2

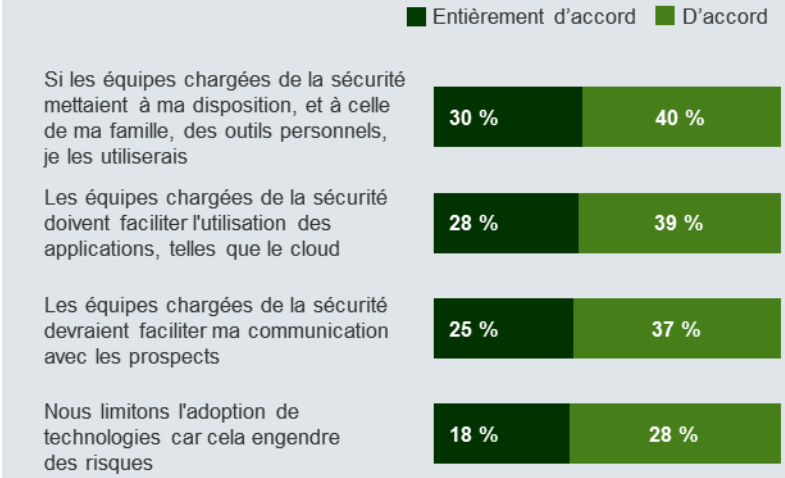
Les équipes chargées de la sécurité peuvent devenir un facilitateur de personnel si elles proposent les bons outils

La diversité de la technologie et l'évolution des méthodes de travail des employés conduisent à de nombreux problèmes de sécurité qui menacent la marque et la sécurité de votre entreprise. Par exemple, le besoin accru des employés concernant l'accès aux applications et aux données poussera les équipes chargées de la sécurité à garantir que la nouvelle technologie du personnel ne met pas en danger les informations sensibles, tout en conférant aux employés autorisés un libre accès, que leur entreprise possède ou non les appareils qu'ils utilisent.

Il n'est donc pas surprenant que les employés souhaitent obtenir des outils de sécurité personnels (70 %) et un accès aux applications dans le cloud (67 %). Fournir des outils de sécurité à tous les types d'employés permet à ceux-ci de se montrer plus vigilants lorsqu'ils accèdent à des informations sensibles.

Les entreprises qui recherchent des solutions de sécurité permettant aux employés de collaborer efficacement et en toute sécurité assureront leur protection sur le long terme. Pour améliorer la sécurité sans nuire à la productivité et aux résultats commerciaux, les professionnels de la sécurité doivent permettre aux employés de se prendre en charge avec de meilleurs outils et conseils. Le rôle des équipes chargées de la sécurité informatique doit consister à faire confiance, mais aussi à vérifier.

« À quel point êtes-vous d'accord avec les affirmations suivantes concernant les équipes chargées des protocoles de sécurité sur les appareils que vous utilisez pour travailler ? » (Seules les réponses « Entièrement d'accord » et « D'accord » sont affichées)



Panel : 400 travailleurs de l'information de tous secteurs d'activité aux États-Unis, au Royaume-Uni, en Inde et en Australie
Source : étude réalisée par Forrester Consulting pour Dell en septembre 2017.

Technology Adoption Profile personnalisé pour Dell | Octobre 2017

Sécurité évolutive adaptée à l'employé moderne

Prise en compte de tous les employés : besoins de sécurité pour une meilleure expérience des employés

La technologie transforme les méthodes et le lieu de travail des employés. Les équipes chargées de la sécurité doivent tenir le rythme et s'adapter à tous les types d'employés. L'étude a permis de tirer trois conclusions clés :

› **Les équipes chargées de la sécurité doivent servir et protéger les employés ne travaillant pas dans un bureau.** D'une part, les employés de bureau présentent des exigences moins élevées en termes de sécurité et sont moins exposés aux risques, étant donné qu'ils sont protégés par l'établissement ou le bureau dans lequel ils travaillent. D'autre part, les employés ne travaillant pas dans un bureau et les professionnels chargés la propriété intellectuelle sont plus susceptibles d'être négligés. Les entreprises doivent également s'adapter à leurs besoins et reconnaître qu'une approche universelle ne fonctionnera pas pour tout le monde.

› **Les travailleurs de l'information contournent les procédures de sécurité pour être productifs, sans intention malveillante.** L'environnement numérique actuel exige une certaine réactivité de la part des employés. Évidemment, les procédures de sécurité ne sont pas conçues pour leur faciliter le travail, c'est notamment le cas pour les employés ne travaillant pas dans le bureau de leur entreprise. Afin d'obtenir ce qu'ils veulent, quand cela est nécessaire pour mieux servir les clients, ils contournent les politiques de sécurité.

› **Les habitudes des employés amplifient les mauvaises pratiques de sécurité.** Différents types de profils effectueront leur travail d'une manière naturelle, inhérente à leur rôle. Par exemple, les employés ne travaillant pas dans un bureau et les professionnels chargés de la propriété intellectuelle doivent partager des données avec des collègues et des personnes tierces sur une clé USB ou un CD, même si ceux-ci risquent d'être perdus. En d'autres termes, le risque réside dans l'appareil non sécurisé, et les habitudes de travail l'amplifient.

MÉTHODOLOGIE

Ce Technology Adoption Profile a été réalisé pour Dell. Les questions de cette enquête personnalisée ont été posées à 400 travailleurs de l'information issus de tous les secteurs d'activité en Australie, en Inde, au Royaume-Uni et aux États-Unis.

L'enquête personnalisée a commencé en juillet 2017 et s'est achevée en octobre 2017. Pour plus d'informations sur le panel de données et les services Tech Industry Consulting de Forrester, visitez le site Forrester.com.

Directeur de projet

Tarun Avasthy
Consultant sur l'impact marché